

1    CLAIMS

2    What is claimed is:

3    *Sub*  
4    *a* 1. A method for generating a key pair, the method  
comprising:

5            - forming a private key which includes at least  
6    one enhancing key; and  
7            - forming a public key which includes a commitment  
8    to said at least one enhancing key, wherein the public  
9    key and the private key form the key pair.

10   2. The method as recited in Claim 1, wherein the step  
11   of forming a public key comprises computing a function  
12   on a commitment to an enhancing key and a 1-time public  
13   key.

14   3. The method as recited in Claim 1, wherein the  
15   enhancing key is randomly chosen.

16   4. The method as recited in Claim 1, further comprising  
17   employing the enhancing key in a process.

18   5. A method as recited as in Claim 4, wherein the  
19   process performs a hash calculation.

1 6. A method as recited in Claim 1, further comprising  
2 computing a certificate for the public key.

3 7. A method as recited as in Claim 1, wherein the  
4 commitment is a TCR commitment.

5 8. The method as recited in Claim 7, further comprising  
6 employing the enhancing key in a process.

7

8 9. A computer program product comprising a computer  
9 usable medium having computer readable program code  
10 means embodied therein for generating a key pair, the  
11 computer readable program code means in said computer  
12 program product comprising computer readable program  
13 code means for causing a computer to effect the steps  
14 of claim 1.

15 10. A method of forming a TCR commitment comprising:  
16 - providing a commitment for a first string, and  
17 - applying a TCR function to a second string that  
18 includes the commitment.

19 11. A method as recited in Claim 10, wherein the step  
20 of applying includes:  
21 - choosing a random key for the TCR function.  
22 - evaluating the TCR function on the random key and  
23 the second string.

1 12. A method as recited in Claim 11, wherein the TCR  
2 function is a basic cryptographic primitive.

3 13. A method as recited in Claim 12, wherein the  
4 cryptographic primitive is the SHA-1 compress function.

5 14. A method as recited in Claim 10, wherein the step  
6 of applying forms a TCR function output which is 80  
7 bits long.

8 15. An article of manufacture comprising a computer  
9 usable medium having computer readable program code  
10 means embodied therein for generating a key pair, the  
11 computer readable program code means in said article of  
12 manufacture comprising computer readable program code  
13 means for causing a computer to effect the steps of  
14 claim 1.

15 16. A method as recited in Claim 10, further comprising  
16 employing the TCR commitment in an enhanced commitment  
17 based signature scheme.

18 17. A method as recited in Claim 1, wherein the  
19 public-private key pair is used a bounded number of  
20 times.

21 18. A method as recited in Claim 17, where the bounded  
22 number is 36.

1 19. A method as recited in Claim 12, wherein the TCR  
2 function is a TCR hash tree based on a basic  
3 cryptographic primitive.

4 20. A method as recited in Claim 1, further comprising  
5 employing the key pair in a commitment based signature  
6 scheme.

7 21. The method as recited in Claim 4, wherein the  
8 process is a 36-time signature scheme.

9 22. A method as recited in Claim 10, further  
10 comprising employing the TCR commitment in an  
11 E-commerce protocol.

12 23. A method comprising:

13 generating a TCR commitment opening function for  
14 extracting a data string committed to by at least one  
15 TCR commitment message,

16 utilizing a corresponding TCR opening string for each  
17 said at least one TCR commitment message, and

18 employing a TCR function and a regular commitment  
19 scheme used in generating said at least one TCR  
20 commitment message and used in generating said  
21 corresponding TCR opening string.

1 24. An article of manufacture comprising a computer  
2 usable medium having computer readable program code  
3 means embodied therein for generating a TCR commitment  
4 opening function for extracting a data string committed  
5 to by at least one TCR commitment message,, the  
6 computer readable program code means in said article of  
7 manufacture comprising computer readable program code  
8 means for causing a computer to effect the steps of  
9 claim 23.

10 25. A computer program product comprising a computer  
11 usable medium having computer readable program code  
12 means embodied therein for causing generation of a TCR  
13 commitment opening function, the computer readable  
14 program code means in said computer program product  
15 comprising computer readable program code means for  
16 causing a computer to effect the steps of claim 23.

17 26. A method as recited in Claim 25, wherein the step  
18 of generating the TCR commitment function includes:

19 receiving a data string to be committed and  
20 receiving secret information if any in said regular  
21 commitment scheme;

22 computing a regular commitment message using said  
23 regular commitment scheme upon both said data string  
24 and said secret information;

1 randomly selecting a key for said TCR function;

2 computing said TCR function on said key and said  
3 regular commitment message and obtaining a resulting  
4 hash value;

5 forming a TCR commitment message including said  
6 resulting hash value and said key, said TCR commitment  
7 message being an output of said TCR commitment  
8 function.

9 27. A method as recited in Claim 26, further  
10 comprising saving said regular commitment message.

11 28. A method as recited in Claim 27, wherein the step  
12 of saving is performed for a commiter.

13 29. A method comprising:

14 generating a TCR de-commitment function for  
15 de-committing at least one TCR commitment message  
16 employing a TCR function and a regular commitment  
17 scheme used in generating said at least one TCR  
18 commitment message.

19 30. A method as recited in Claim 29, wherein the step  
20 of generating the TCR de-commitment function includes:

1 receiving a data string committed and receiving  
2 secret information used in generating said at least one  
3 TCR commitment message if any;

4 receiving a regular commitment message computed as  
5 part of generation of said at least one TCR commitment  
6 message;

7 computing the regular de-commitment function on  
8 using said regular commitment message, said data string  
9 and said secret information and generating a regular  
10 opening string;

11 forming a TCR opening string including said  
12 regular opening string and said regular commitment  
13 message, said TCR opening string being an output of  
14 said TCR de-commitment function.

15 31. A method comprising:

16 generating a TCR commitment function by employing any  
17 TCR function and utilizing any regular commitment  
18 scheme.

19 32. A method as recited in Claim 23, wherein the step  
20 of generating the TCR commitment opening function  
21 includes:

1 receiving a TCR commitment message and a  
2 corresponding TCR opening string;

3 extracting a hash value and a key from said TCR  
4 commitment message; and

5 extracting a regular opening string and a regular  
6 commitment message from said corresponding TCR opening  
7 string

8 computing the TCR hash function with said key and  
9 said regular commitment message forming a result  
10 value; and

11 comparing said result value with said hash value.

12 33. A method as recited in Claim 32, further  
13 comprising reporting an error if the step of comparing  
14 results in a non-compare, and reporting a non-error if  
15 the step of comparing results in a compare.

16 34. A method as recited in Claim 32, if the step of  
17 comparing results in a compare, further comprising  
18 applying said regular opening commitment function on  
19 said regular opening string and said regular commitment  
20 message to produce said data string,.

21 35. A method comprising:

1 constructing a TCR commitment scheme comprising:

- 2                    a TCR commitment function;
- 3                    a TCR de-commitment function; and
- 4                    a TCR commitment opening function,

5 by employing any TCR function and any regular  
6 commitment scheme.

7 36. An article of manufacture comprising a computer  
8 usable medium having computer readable program code  
9 means embodied therein for generating a TCR commitment  
10 function, the computer readable program code means in  
11 said article of manufacture comprising computer  
12 readable program code means for causing a computer to  
13 effect the step of claim 25.

14 37. A method as recited in Claim 25, wherein the TCR  
15 function is a basic cryptographic primitive.

16 38. A method as recited in Claim 37, wherein the  
17 cryptographic primitive is the SHA-1 compress function.

18 39. A method as recited in Claim 26, wherein said  
19 resulting hash value is 80 bits long.

20 40. A method as recited in Claim 25, wherein the TCR  
21 function is a TCR hash tree based on a basic  
22 cryptographic primitive.

1 41. A method as recited in Claim 35, further  
2 comprising employing the TCR commitment scheme in an  
3 enhanced commitment based signature scheme.

4 42. A method as recited in Claim 35, further  
5 comprising employing the TCR commitment scheme in an  
6 E-commerce protocol.

7 43. An article of manufacture as recited in claim 42,  
8 wherein the step of generating the TCR commitment  
9 function includes:

10 receiving a data string to be committed and  
11 receiving secret information if any in said regular  
12 commitment scheme;

13 computing a regular commitment message using said  
14 regular commitment scheme upon both said data string  
15 and said secret information;

16 randomly selecting a key for said TCR function;

17 computing said TCR function on said key and said  
18 regular commitment message and obtaining a resulting  
19 hash value;

20 forming a TCR commitment message including said  
21 resulting hash value and said key, said TCR commitment

1 message being an output of said TCR commitment  
2 function.

3 44. An article of manufacture comprising a computer  
4 usable medium having computer readable program code  
5 means embodied therein for generating a TCR  
6 de-commitment function, the computer readable program  
7 code means in said article of manufacture comprising  
8 computer readable program code means for causing a  
9 computer to effect the steps of claim 29.